


[Subscribe \(Full Service\)](#) [Register \(Limited Service, Free\)](#) [Login](#)

 Search: ☒ The ACM Digital Library ☐ The Guide

THE ACM DIGITAL LIBRARY


[Feedback](#) [Report a problem](#) [Satisfaction survey](#)

 Terms used one time password biometric

Found 26 of 157,956

Sort results by


[Save results to a Binder](#)
[Try an Advanced Search](#)

Display results


[Search Tips](#)

 Try this search in [The ACM Guide](#)
☐ Open results in a new window

Results 1 - 20 of 26

 Result page: [1](#) [2](#) [next](#)

 Relevance scale ☐ ☐ ☐ ☐ ☐

1 [Staying connected: Let your fingers do the talking](#)

Meg McGinity

 January 2005 **Communications of the ACM**, Volume 48 Issue 1

 Full text available: [pdf\(63.56 KB\)](#) [html\(14.42 KB\)](#) Additional Information: [full citation](#), [abstract](#), [index terms](#)

Biometrics is pointing its way into everyday applications. But figuring out how it fits into telecom and wireless services, never mind society, might just get downright touchy.

2 [Quality of security service](#)

Cynthia Irvine, Timothy Levin

 February 2001 **Proceedings of the 2000 workshop on New security paradigms**

 Full text available: [pdf\(684.54 KB\)](#) Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)

Keywords: quality of security service, quality of service, security range, variant security

3 [Assurance in life/nation critical endeavors: Biometrics or ... biohazards?](#)

John Michael Williams

 September 2002 **Proceedings of the 2002 workshop on New security paradigms**

 Full text available: [pdf\(1.17 MB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#), [review](#)

IPSE DIXIT Biometrics as an array of deployable technologies presumes an elaborate infrastructure, including underlying science that justifies its claims of detection, classification, identification and authentication of individual human identities; particularly of those who are runaways, illegal immigrants, fugitives, criminals, terrorists, and so on. This will now too often be literally a matter of life and death, both for the public and the individuals identified. The "New Security Paradigm" em ...

4 [ID-based password authentication scheme using smart cards and fingerprints](#)

Hyun-Sung Kim, Sung-Woon Lee, Kee-Young Yoo

 October 2003 **ACM SIGOPS Operating Systems Review**, Volume 37 Issue 4

 Full text available: [pdf\(466.31 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#)

This paper proposes two ID-based password authentication schemes, which does not

require a dictionary of passwords or verification tables, with smart card and fingerprint. In these schemes, users can change their passwords freely. For a network without synchronization clocks, the proposed nonce-based authentication scheme can withstand message replay attacks. The proposed two schemes require a system to authenticate each user by each user's knowledge, possession, and biometrics, and this feature ...

Keywords: ID-based scheme, fingerprint, password authentication, smart card

5 Voice biometrics

Judith A. Markowitz

September 2000 **Communications of the ACM**, Volume 43 Issue 9

Full text available:  [pdf\(240.49 KB\)](#)
 [html\(36.88 KB\)](#)

Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)



6 Protecting applications with transient authentication

Mark D. Corner, Brian D. Noble

May 2003 **Proceedings of the 1st international conference on Mobile systems, applications and services**

Full text available:  [pdf\(294.40 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#)

How does a machine know who is using it? Current systems authenticate their users infrequently, and assume the user's identity does not change. Such *persistent authentication* is inappropriate for mobile and ubiquitous systems, where associations between people and devices are fluid and unpredictable. We solve this problem with *Transient Authentication*, in which a small hardware token continuously authenticates the user's presence over a short-range, wireless link. We present the fo ...



7 Written on the body: biometrics and identity

Irma van der Ploeg

March 1999 **ACM SIGCAS Computers and Society**, Volume 29 Issue 1

Full text available:  [pdf\(895.43 KB\)](#) Additional Information: [full citation](#), [index terms](#)



8 National id card: the next generation: The US/Mexico border crossing card (BCC): a case study in biometric, machine-readable id

Andrew Schulman

April 2002 **Proceedings of the 12th annual conference on Computers, freedom and privacy**

Full text available:  [htm\(187.31 KB\)](#) Additional Information: [full citation](#), [index terms](#)



9 Response to "Problems with DCE security services"

Walter Tuvell

April 1996 **ACM SIGCOMM Computer Communication Review**, Volume 26 Issue 2

Full text available:  [pdf\(1.01 MB\)](#) Additional Information: [full citation](#), [index terms](#)




10 BITS: a smartcard protected operating system

Paul C. Clark, Lance J. Hoffman



November 1994 **Communications of the ACM**, Volume 37 Issue 11

Full text available:  [pdf\(3.80 MB\)](#)

Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)

11 Problems with DCE security services

Gregory White, Udo Pooch

October 1995 **ACM SIGCOMM Computer Communication Review**, Volume 25 Issue 5

Full text available:  [pdf\(479.39 KB\)](#)

Additional Information: [full citation](#), [abstract](#), [index terms](#)

Distributed computing is receiving an ever increasing amount of interest and with it come many challenges, not the least of which is how to maintain system and network security. Issues relating to user authentication, access authorization, and communication security must be addressed when multiple, heterogeneous systems are connected. While these issues have been addressed in OSFs DCE, several problems remain. This paper describes some of these problems.

12 Modern trends in authentication

David L. Lipton, Harry K. T. Wong

September 1985 **ACM SIGSAC Review**, Volume 3 Issue 2-4

Full text available:  [pdf\(517.65 KB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#)

Authentication is the process of verifying a person's claim of identity. The designers of secure computer systems have incorporated many techniques of user-validation from law enforcement, from industrial security, and from the financial community. Several methods have also been developed explicitly for use in computer systems. This paper will present an overview of all methods of authentication currently used in computer security. Implementation considerations will also be discussed.

13 Commercial key recovery

Stephen T. Walker, Steven B. Lipner, Carl M. Ellison, David M. Balenson

March 1996 **Communications of the ACM**, Volume 39 Issue 3

Full text available:  [pdf\(536.19 KB\)](#)

Additional Information: [full citation](#), [references](#), [index terms](#), [review](#)

14 Access management for distributed systems: Peer-to-peer access control architecture using trusted computing technology

Ravi Sandhu, Xinwen Zhang

June 2005 **Proceedings of the tenth ACM symposium on Access control models and technologies**

Full text available:  [pdf\(215.48 KB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

It has been recognized for some time that software alone does not provide an adequate foundation for building a high-assurance trusted platform. The emergence of industry-standard trusted computing technologies promises a revolution in this respect by providing roots of trust upon which secure applications can be developed. These technologies offer a particularly attractive platform for security in peer-to-peer environments. In this paper we propose a trusted computing architecture to enforce ac ...

Keywords: access control, policy enforcement, security architecture, trusted computing

15 On-line e-wallet system with decentralized credential keepers

Stig Frode Mjølunes, Chunming Rong

February 2003 **Mobile Networks and Applications**, Volume 8 Issue 1

Full text available:  [pdf\(240.23 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)


We propose a generalization of the architecture of an electronic wallet, as first developed in the seminal European research project CAFE. With this model you can leave most of the content of your electronic wallet at the security of your residential electronic keeper, while roaming with your favorite mobile terminals. Emerging mobile handsets with both short range Bluetooth and cellular GPRS communications provide a sufficient communication platform for this electronic wallet architecture. Howe ...

Keywords: digital credentials, e-wallet architecture, mobile commerce, payment protocols, privacy

16 Intrusion detection in wireless ad-hoc networks

Yongguang Zhang, Wenke Lee

August 2000 **Proceedings of the 6th annual international conference on Mobile computing and networking**

Full text available:  [pdf\(936.44 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

As the recent denial-of-service attacks on several major Internet sites have shown us, no open computer network is immune from intrusions. The wireless ad-hoc network is particularly vulnerable due to its features of open medium, dynamic changing topology, cooperative algorithms, lack of centralized monitoring and management point, and lack of a clear line of defense. Many of the intrusion detection techniques developed on a fixed wired network are not applicable in this new environment. Ho ...

17 Intrusion detection techniques for mobile wireless networks

Yongguang Zhang, Wenke Lee, Yi-An Huang

September 2003 **Wireless Networks**, Volume 9 Issue 5

Full text available:  [pdf\(164.73 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

The rapid proliferation of wireless networks and mobile computing applications has changed the landscape of network security. The traditional way of protecting networks with firewalls and encryption software is no longer sufficient and effective. We need to search for new architecture and mechanisms to protect the wireless networks and mobile computing application. In this paper, we examine the vulnerabilities of wireless networks and argue that we must include intrusion detection in the security ...

Keywords: anomaly detection, cooperative detection, intrusion detection, intrusion response, mobile ad-hoc networks

18 Features: Security is Harder than You Think

John Viega, Matt Messier

July 2004 **Queue**, Volume 2 Issue 5

Full text available:  [pdf\(982.74 KB\)](#)  [html \(19.45 KB\)](#) Additional Information: [full citation](#), [index terms](#)

19 A smartcard for authentication in WLANs

Marc Loutrel, Pascal Urien, Guy Pujolle

October 2003 **Proceedings of the 2003 IFIP/ACM Latin America conference on Towards**

a Latin American agenda for network research

Full text available:  pdf(333.05 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)



Wireless LANs based on the IEEE 802.11b standard have spread very quickly over the past few years. Nevertheless a lot of security issues remain and stop its deployment in corporations. One of the most important issues is the authentication of a terminal to an Access Point. We propose an interface to integrate the Extensible Authentication Protocol into smartcards and will show that smartcards could constitute the de-facto device for authentication in Wireless LAN as they are for GSM and will ...

Keywords: authentication, smartcard, wireless LANs

20 Payments and banking with mobile personal devices

Amir Herzberg

May 2003 **Communications of the ACM**, Volume 46 Issue 5

Full text available:  pdf(152.82 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#), [review](#)
 html(31.60 KB)

Mobile devices enable secure, convenient authorization of e-banking, retail payment, brokerage, and other types of transactions.

Results 1 - 20 of 26

Result page: **1** [2](#) [next](#)

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2005 ACM, Inc.

[Terms of Usage](#) [Privacy Policy](#) [Code of Ethics](#) [Contact Us](#)

Useful downloads:  [Adobe Acrobat](#)  [QuickTime](#)  [Windows Media Player](#)  [Real Player](#)

WEST Search History

DATE: Friday, July 08, 2005

Hide?	Set Name	Query	Hit Count
	<i>DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=OR</i>		
<input type="checkbox"/>	L47	L42 and "one-time password"	2
<input type="checkbox"/>	L46	L45 and "one-time"	3
<input type="checkbox"/>	L45	L44 and "firewall"	12
<input type="checkbox"/>	L44	L43 and "SSL"	18
<input type="checkbox"/>	L43	L42 and "password"	159
<input type="checkbox"/>	L42	709/250.ccls.	1378
<input type="checkbox"/>	L41	L40 and "SSL"	0
<input type="checkbox"/>	L40	709/250.pn.	0
<input type="checkbox"/>	L39	20010055388	3
<input type="checkbox"/>	L38	L37 and "proxy"	24
<input type="checkbox"/>	L37	L36 and "SSL"	24
<input type="checkbox"/>	L36	L35 and "fingerprint"	25
<input type="checkbox"/>	L35	L34 and "encrypt"	25
<input type="checkbox"/>	L34	L33 and "firewall"	25
<input type="checkbox"/>	L33	L31 and "hash"	26
<input type="checkbox"/>	L32	L31 and "hash value"	1
<input type="checkbox"/>	L31	"one-time password" same "biometrics"	40
<input type="checkbox"/>	L30	L29 and "value hash"	4
<input type="checkbox"/>	L29	"one-time password" and "authentication server"	144
<input type="checkbox"/>	L28	L27 and "hash value"	10
<input type="checkbox"/>	L27	L26 and "biometric"	183
<input type="checkbox"/>	L26	"one-time password"	568

END OF SEARCH HISTORY

WEST Search History

[Hide Items](#)[Restore](#)[Clear](#)[Cancel](#)

DATE: Friday, July 08, 2005

Hide?	Set Name	Query	Hit Count
		<i>DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=OR</i>	
<input type="checkbox"/>	L38	L37 and "proxy"	24
<input type="checkbox"/>	L37	L36 and "SSL"	24
<input type="checkbox"/>	L36	L35 and "fingerprint"	25
<input type="checkbox"/>	L35	L34 and "encrypt"	25
<input type="checkbox"/>	L34	L33 and "firewall"	25
<input type="checkbox"/>	L33	L31 and "hash"	26
<input type="checkbox"/>	L32	L31 and "hash value"	1
<input type="checkbox"/>	L31	"one-time password" same "biometrics"	40
<input type="checkbox"/>	L30	L29 and "value hash"	4
<input type="checkbox"/>	L29	"one-time password" and "authentication server"	144
<input type="checkbox"/>	L28	L27 and "hash value"	10
<input type="checkbox"/>	L27	L26 and "biometric"	183
<input type="checkbox"/>	L26	"one-time password"	568

END OF SEARCH HISTORY